Listing of the Claims:

The text of all claims under examination is submitted, and the status of each is identified. This listing of claims replaces all prior versions, and listings, of claims in the application.

1. (Currently Amended) A computer-implemented method employing a microprocessor for controlling access to a document, the method comprising:

determining, using the microprocessor, an access right for a user;

building a member definition comprising a member identifier, an access control list comprising a list of access rights of the user, a private key of a key pair for use in encrypting the document, and a digital signature, and associating the member definition with the user;

linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion,

receiving a request from the user to access the document;

comparing the request with the access right; [[and]]

allowing access to only the first data portion in accordance with the access right; and

denying access to the second data portion in accordance with the access right, wherein the denying access comprises at least one of logging information regarding the denial of access of access to the second data portion, and notifying security personnel regarding the denial of access to the second data portion.

2. (Canceled)

3. (Canceled)

4. (Original) The method of claim 1, further comprising adding a new user to the document.

5. (Original) The method of claim 1, further comprising removing a member from the document.

6. (Original) The method of claim 1, further comprising:

storing the member definition remotely from the document.

7. (Original) The method of claim 1, further comprising:
storing the member definition in the document.

8. (Original) The method of claim 1, further comprising:
encrypting the document; and
linking the member definition with a public key and a private key.

9. (Original) The method of claim 1, further comprising:
determining a second access right for the user;
building a second member definition using the second access right; and
linking the second member definition to a second portion of a document.

10. (Original) The method of claim 9, wherein the first portion of the document and the second portion of the document are different.

11. (Currently Amended) A computer-implemented system for controlling access to a document, comprising:
a microprocessor;
memory accessible by the microprocessor;
a document comprising a first data and a second data;
a first member definition associated with the first data, wherein the first member definition contains a first user identifier, a private key of a first key pair for use in encrypting the first data, and a first access right for a first user for the first data;
a second member definition associated with the second data, wherein the second member definition contains a second user identifier, a private key of a second key pair for use in encrypting the second data, and a second access right for a second user for the second data; and
an access controller that receives a request from the first user for access to the document, wherein the access controller locates the first member definition and allows access to the first data only and

denies access to the second data, wherein the denying access comprises at least one of logging information regarding the denial of access to the second data, and notifying security personnel regarding the denial of access to the second data.

12. (Original) The system of claim 11, wherein the access controller limits access to the document in accordance with the first access right and the second access right.

13. (Original) The system of claim 11, wherein the first user identifier and the second user identifier identify the same user and the first access right and the second access right identify different access rights.

14. (Original) The system of claim 11, wherein the first member definition contains a digital signature.

15. (Original) The system of claim 11, wherein the first member definition and second member definition are stored remotely from the document.

16. (Original) The system of claim 11, wherein the first member definition and second member definition are stored in the document.

17. (Original) The system of claim 11, wherein the document is a tagged document.

18. (Original) The system of claim 11, wherein the document is an XML document.

19. (Original) The system of claim 11, wherein the document is a text document.

20. (Original) The system of claim 11, wherein the document is a binary document.

21. (Currently Amended) A non-transitory computer-readable storage medium comprising a plurality of instructions for execution by at least one computer processor, wherein the instructions are for:

determining a first access right for a first user and a second access right for a second user;

building a first member definition comprising the first access right, a first user identifier, a private key of a first key pair for enabling the first user to encrypt a first portion of a document, and a first digital signature;

building a second member definition comprising the second access right, a second user identifier, a private key of a second key pair for enabling the second user to encrypt a second portion of the document, and a second digital signature;

linking the first member definition to the first portion of the document;

linking the second member definition to the second portion of the document;

storing the first member definition and second member definition remotely from the document;

encrypting the document;

receiving a request from a requester to access the document;

based on the first user identifier and the second user identifier, determining the access right for the requester for the first portion of the document and the second portion of the document; and

allowing access only to the first portion of the document and denying access to the second portion in accordance with the first access right, or allowing access only to the second portion of the document and denying access to the first portion in accordance with the second access right, wherein the denying access comprises at least one of logging information regarding the denial of access, and notifying security personnel regarding the denial of access.